## REMARKS/ARGUMENTS

Upon entry of this Amendment, which amends Claims **1, 7, 27**, Claims 1-27 remain pending in the present application.

In the July 15, 2005 Office Action, Claims 1-8, 10-14, 16-18, 20 , 21, 26 and 27 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,003,135 to Bialick et al. (hereinafter referred to as "Bialick et al."). Claims 9 and 22-25 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bialick et al. in view of U.S. Patent No. 6,374,315 to Okada et al. (hereinafter referred to as "Okada et al."). Claims 15 and 19 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Howard in view of Chiles et al. and Ferchau et al. Finally, Claim 15 was rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bialick et al. in view of U.S. Patent No. 6,134,593 to Alexander et al. (hereinafter referred to as "Alexander et al.").

Applicant respectfully requests reconsideration of the claims in view of the above amendments and the comments below.

### *35 U.S.C. § 102(b) Claim Rejections – Claims 1-8, 10-14, 16-18, 20 , 21, 26 and 27*

On pages 2-7 of the July 15, 2005 Office Action, Claims 1-8, 10-14, 16-18, 20 , 21, 26 and 27 were rejected as allegedly being anticipated by Bialick et al. For the following reasons Applicant respectfully disagrees.

Bialick et al. discloses a modular device that communicates with a host computing device and enables security operations to be performed by the modular device

on: (i) data stored within the host computing device, (ii) data provided from the host computing device to the modular device, or data retrieved by the host computing device from the modular device. The modular device includes a security module that is adapted to enable performance of the security operations on the data and a target module that is adapted to enable a defined interaction with the host computing device. The target module can be embodied by any of a variety of modules having different types of functionality (e.g. data storage, data communication, data input and output, user identification).

By contrast, independent Claim 1 of the present application claims a method that includes "checking a wireless network card for a stored platform discrimination indication" and, "depending on a value of the platform discrimination indication, inhibiting or allowing data transfer using the wireless network card." Comparing independent Claim 1 of the present application to Bialick et al. reveals the following important distinctions. Applicant respectfully believes that these distinctions demonstrate that Bialick et al. cannot be properly maintained to support the rejection of Claim 1.

First, Bialick et al. fails to teach "checking a wireless network card for a stored platform discrimination indication." Despite this, in the Office Action it is asserted that such subject matter is taught in col. 2, lines 32-47; col. 9, line 45 through col. 10, line 10; and col. 13, lines 11-61. Applicant respectfully disagrees.

Col. 2, lines 32-47 of Bialick et al. describes a prior art approach to encrypting data stored on a host computing device 201, before that data is sent to a portable device 202. According to that prior art approach, data from the host computing device is first

transferred from the host computing device 201 to a security device 203, which encrypts the data. The encrypted data is then transferred from the security device back to the host computing device, which responds by transferring the encrypted data to portable device 202. Nothing in this excerpt teaches "checking a wireless network card for a stored platform indication."

Col. 9, line 45 through col. 10, line 10 of Bialick et al. describes detecting the presence of a new peripheral (i.e. "modular") (col. 9, lines 45-50); identifying the type of peripheral device according to previous approaches (col. 9, lines 51-65); and suspending the peripheral device identification process used by the previous approaches, so that the modular device can first establish its own identify (col. 9, line 65 through col. 10, line 3). The ability of the modular device to identify itself enables the modular device to assume the identity of a target module that is part of the modular device (col. 10, lines 4-10). Again, there is nothing in these excerpts teaching "checking a wireless network card for a stored platform indication," as independent Claim 1 of the present application recites. Indeed, there is absolutely no reference at all to any idea of "platform discrimination," let alone of a "platform discrimination indication" stored in a "wireless network card."

Finally, col. 13, lines 11-61 of Bialick et al. discusses how a driver of the disclosed modular device determines whether data stored in a predetermined location of a memory device of the modular device identifies whether the modular device is a device having security functionality that is compatible with the modular device driver. This excerpt only describes a determination of whether a modular device has security functionality that is compatible with a driver of the modular device. The determination

does not depend on the type of platform in which the modular device is associated. Rather, the description only describes a determination as to whether the modular device has security functionality that is compatible with the driver of the modular device. Accordingly, as with all of the other excerpts referenced in the Office Action, this excerpt provides no teaching of "platform discrimination" or of "checking a wireless network card for a stored platform discrimination indication."

In addition to not teaching "checking a wireless network card for a stored platform discrimination indication," Bialick et al. also fails to teach, "depending on a value of the platform discrimination indication, inhibiting or allowing data transfer using the wireless network card." As explained above, Bialick et al. does not disclose a wireless network card that stores a "platform discrimination indication." Since it does not, it is impossible for the reference to teach inhibiting or allowing data transfer "depending on a value of the platform discrimination indication," as independent Claim 1 of the present application recites.

It should be mentioned here that, even if Bialick et al. disclosed a wireless network card that stored a "platform discrimination indication," the excerpts of Bialick cited in the Office Action do not teach "depending on a value of the platform discrimination indication, inhibiting or allowing data transfer using the wireless network card," as independent Claim 1 of the present application recites. Specifically, col. 6, lines 46-53 of Bialick et al. merely describes how the disclosed modular device includes a security module that enables security operations on data stored on a host computing device, data transmitted from the host computing device to the modular device, or data

transmitted from the modular device to the host computing device. Col. 10, lines 26-49 merely describe how the operating system of the host computing device can identify the type of peripheral (i.e. modular) device by accessing a known memory section of a memory device of the peripheral device. The data accessed is referred to in col. 10, lines 47-49 as "modular device identification data." Not only is data transfer using a wireless network card not even mentioned in these excerpts, there is nothing in the excerpts that relates to "platform discrimination," or to "inhibiting or allowing data transfer using the wireless network card" "depending on a value of the platform discrimination indication."

For at least the foregoing reasons, Applicant believes that the rejection of independent Claim 1 as being anticipated by Bialick et al. cannot be properly maintained. Applicant requests, therefore, that the rejection be withdrawn.

In the Office Action, independent Claim 10 of the present application was also rejected for allegedly being anticipated by Bialick et al. For the following reasons, Applicant respectfully disagrees with this rejection.

Claim 10 claims a method that uses "an input electronic ID of a wireless network card to determine a first key value," which is performed at "a first device" that is not the same as the later recited "portable data device." In the Office Action, the host computing device 311 of Bialick et al. is described as corresponding to the "first device." However, there is no teaching that the host computing device 311 in Bialick et al. uses "an input electronic ID of a wireless network card to determine a first key value." Despite this, in the Office Action it is asserted that col. 18, lines 48-59; col. 14, lines 3-18; and col. 21,

lines 28-50 do teach such subject matter. For the following reasons, Applicant respectfully disagrees.

Col. 18, lines 48-59 describe how a specific embodiment of the disclosed modular device includes only a security module, which may be used to encrypt or decrypt data stored on the host computing device by: receiving the data from the host computing device, encrypting or decrypting the data as appropriate, and then returning the encrypted or decrypted data to the host computing device. It is also described in this excerpt how the security module of the disclosed modular device may be used to encrypt or decrypt data stored on the host computing device, while a target module of the modular device, although also present in the modular device, is not used. There is nothing in this excerpt teaching "using an electronic ID of a wireless network card to determine a first key value," let alone performing such an operation on a "first device" that is different from the separate and later-recited "portable data device."

Col. 14, lines 3-18 of Bialick et al. describes how a user may be required to enter a password or PIN before the user is allowed to use the security functionality of the modular device. While a password or PIN is described in this excerpt, there is nothing in the excerpt that teaches that "an electronic ID of a wireless network card" is used to determine a "first key value."

Finally, col. 21, lines 28-50 of Bialick et al. describe how the disclosed modular device may implement one or more cryptographic key exchange operations. However, again, there is no teaching in this excerpt of "a first device" (which is different than the

later recited "portable data device") "using an input electronic ID of a wireless network card to determine a first key value."

Claim 10 also recites how the "first key value" determined "at [the] first device" is used to "calculate a calculated ID value" at "a portable data device not the first device." In the Office Action, it is asserted that col. 18, lines 57-59 of Bialick et al. teaches such subject matter. Applicant respectfully disagrees. Col. 18, lines 57-59 of Bialick et al. describes how a security module of the disclosed modular device may be used to encrypt or decrypt data stored on the host computing device, while a target module of the modular device, although also present in the modular device, is not used. There is nothing in this excerpt that teaches "using [a] first key value to calculate a calculated ID."

The method of Claim 10 also recites "using the first key value to calculate a calculated ID value." In the Office Action, it is asserted that col. 18, lines 48-59 and col. 21 lines 28-50 teach such subject matter. For the following reasons, Applicant respectfully disagrees.

As described above, col. 18, lines 48-59 of Bialick et al. describes how a specific embodiment of the disclosed modular device includes only a security module, which may be used to encrypt or decrypt data stored on the host computing device by: receiving the data from the host computing device, encrypting or decrypting the data as appropriate, and then returning the encrypted or decrypted data to the host computing device. It is also described in this excerpt how the security module of the disclosed modular device may be used to encrypt or decrypt data stored on the host computing device, while a

target module of the modular device, although also present in the modular device, is not used. As was pointed out above, there is nothing in this excerpt teaching using an electronic ID of a wireless network card to determine a "first key value." Moreover, there is nothing in this excerpt that teaches "using [a] first key value to calculate a calculated ID value." Neither identification (ID) nor generating a first key value from an electronic ID of a wireless network card are even discussed in col. 18, lines 48-59, let alone using a "first key value" to generate a "calculated ID value."

Further, col. 21, lines 28-50 of Bialick et al., which was also discussed above, fails to teach "using [a] first key value [generated from an input electronic ID of a wireless network card] to calculate a calculated ID value." As explained above, while col. 21, lines 28-50 of Bialick et al. describe how the disclosed modular device may implement one or more cryptographic key exchange operations, there is no teaching in this excerpt of "a first device" (which is different than the later recited "portable data device") "using an input electronic ID of a wireless network card to determine a first key value." Further, similar to col. 18, lines 48-59, neither identification (ID) nor generating a first key value from an electronic ID of a wireless network card are even discussed in col. 21, lines 28-50, let alone using a "first key value" to generate a "calculated ID value."

The method of Claim 10 also recites "comparing [a] calculated ID value to [an] electronic ID of the wireless network card, so that if the calculated ID value matches the electronic ID of the wireless network card data transmissions from the portable data device through the wireless network are enabled." In the Office Action, it is asserted that

col. 6, lines 46-53 and col. 21, lines 39-43 teach such subject matter. For the following reasons, Applicant respectfully disagrees.

Col. 6, lines 46-53 of Bialick et al. describe how the disclosed modular device includes a security module that enables security operations on data stored on a host computing device, data transmitted from the host computing device to the modular device, or data transmitted from the modular device to the host computing device. Col. 21, lines 39-43 describe how the modular device disclosed by Bialick et al. can implement digital signature operations. These excerpts do not teach "comparing [a] calculated ID value to [an] electronic ID of the wireless network card," as Claim 10 of the present application recites, let alone making such a comparison "so that if the calculated ID value matches the electronic ID of the wireless network card data transmissions from the portable data device through the wireless network are enabled."

For at least the foregoing reasons, Applicant respectfully believes that the rejection of independent Claim 10 as being anticipated by Bialick et al. cannot be properly maintained. Applicant requests, therefore, that the rejection be withdrawn.

In the Office Action, independent Claim 27 of the present application was also rejected for allegedly being anticipated by Bialick et al. For the following reasons, Applicant respectfully disagrees with this rejection.

As discussed above, Bialick et al. does not disclose a wireless network card software driver for a portable device that implements "checking [a] wireless network card for a platform discrimination indication," "or using platform discrimination indication to determine whether to enable data transfer using the wireless network card."

Claim 27 further recites "if data transfer is not enabled, prompting a user for a key value." These two features (data transfer not being enabled, and prompting a user for a key value) are, according to the Office Action, disclosed in Bialick at col. 13, lines 31 – 34, and col. 14, lines 3 – 18). The first excerpt—col. 13, lines 34—in fact pertains to a software compatibility issue, which Bialick addresses by explaining that if the driver on the host device determines that the modular device does not have security functionality that is compatible with the driver, execution of the driver terminates and use of the modular device is prevented. There is no discussion of the first feature—data transfer not being enabled. Bialick's explanation at col. 13, lines 31 – 34 simply relates to preventing use of the modular device if software compatibility is not present. The second excerpt—col. 14, lines 3 – 18—relates to the requirement of entry of a correct password before the modular device can be used.

Claim 27 further recites

> using the key value to determine a calculated ID value; comparing the calculated ID value to an ID value obtained from wireless network card; if the calculated ID value matches ID value obtained from the wireless network card, modifying the platform discrimination indication in the wireless network card to enable data transfer using the wireless network card.

Bialick does not disclose a platform discrimination indication, and particularly one that is modified in a wireless network card "to enable data transfer using the wireless network card." The Office Action makes reference to col. 21, lines 39 – 43, which relate to the use of a digital signature operation, and to col. 6, lines 45 – 53, which relate to a general description of the Bailick description as discussed above. There is no mention in

Bailick of using a key value to determine an calculated ID value, comparing the calculated ID value to an ID value obtained form the wireless network card, and modifying the platform discrimination indication in the wireless network card to enable data transfer using the wireless network card if the calculated ID value matches the ID value obtained from the wireless network card.

It will be appreciated that, according to the M.P.E.P., a claim is anticipated under 35 U.S.C. § 102 only if each and every claim element is found, either expressly or inherently described, in a single prior art reference.[1] The aforementioned reasons clearly indicate the contrary, and withdrawal of the 35 U.S.C. § 102 rejection based on Bailick is respectfully urged.

***35 U.S.C. § 103(a) Claim Rejections – Claims 9 and 22-25***

On pages 7-10 of the Office Action, Claims 9 and 22-25 were rejected under § 103(a) as allegedly being unpatentable over Bialick et al. in view of Okada et al. For the following reasons, Applicant respectfully disagrees.

Claim 9 depends from Claim 1. However, Okada et al. does not remedy the above-discussed failure of Bialick to teach or suggest the invention of Claim 1, and for this reason at least, the obviousness rejection based on the combination of Bialick and Okada should be withdrawn.

Claim 22 reads as follows:

[1] Manual of Patent Examining Procedure (MPEP) § 2131. See also *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

> 22. A wireless network card for use with portable data devices, the wireless network card including a stored platform discrimination indication, the value of the platform discrimination indication determining whether the wireless network card can be used with a given type of portable data device, one value of the platform discrimination indication allowing the wireless network card to be used with a restricted set of portable data devices, another value of the platform discrimination indication allowing the use of the wireless network card with an expanded set of portable data devices, the expanded set of portable data devices including the restricted set of portable data devices as well as additional portable data devices not included in the restricted set of portable data devices.

The Office Action proposes to combine Bialick and Okada to arrive at the teachings of the presently-claimed invention. Okada is directed to a system enabling information storage on a floppy disk-type medium in lieu of an IC memory card-type medium. This is made possible using an adapter that fits into an IC memory card slot of a host device and transferring the data to and from the floppy-disk medium by way of the adapter. In the col. 7, lines 51 – 67 passage to which the Office Action points, Okada explains that the host uses CIS and CCR register information to determine which of these two media is connected. There is no teaching or suggestion in Okada of a platform discrimination indication allowing a wireless network card to be used with either a restricted set or expanded set of portable devices. In Okada, the host is determining whether the storage medium is of one type or another. In the presently claimed invention, discrimination information relates to the "host" itself—that is, to the platform—and a determination of the nature of the platform with which the peripheral is

to be enabled is what is being made, not the nature of the peripheral itself. This is at best the reverse of what Okada is doing, even disregarding the distinction between storage media, which is the subject of Okada, and wireless network cards, which is the subject of the presently claimed invention.

Moreover, the motivation to combine Okada with Bialick as provided in the Office Action is tenuous. Bialick is directed to security systems, and in particular, to a system for ensuring that information manipulation or transfer from a host device is conducted in a secure manner. Okada is directed to substituting one storage medium for another. The Office Action reasons that one of ordinary skill in the art would have been motivated to modify the teachings of Okada within the system of Bialick because "it'd restrict/discriminate the wireless network card to be used in certain wireless devices in order to charge the notebook user less amount (for less traffic) than laptop user." However, in Bialick there is mention of dual network card usage—only of usage of an external security system for a host device, possibly with a single network card. Further, there is no mention of the issue of charging a user for anything, much less charging users based on what kind of transmission are being made. Therefore there would be no need to discriminate between dual network cards, or between cards usable with dual devices such as a laptop and personal digital assistant. It appears that the reasoning provided in the Office Action for making the combination of Bialick and Okada is derived from a reading of applicant's own invention, clearly relying on impermissible hindsight. The background section of the applicant's specification discusses determining whether there is authorization to use the wireless network card for transmission of laptop data or PDA

data. It is this reasoning that the Office Action uses to justify the combination of the two references, rather than any reasoning provided in the references themselves, which is absent because the two references are directed to different technologies, address different problems, and lack the basic components necessary to arrive at the presently claimed invention even if their combination were proper. It will be appreciated that According to the Manual of Patent Examining Procedure (M.P.E.P.), in order to establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.[2] The foregoing discussion is clearly indicative of the contrary, and the obviousness rejection based on Bialick and Okada is therefore improper and should be withdrawn.

### *35 U.S.C. § 103(a) Claim Rejections – Claims 15 and 19*

On page 11 of the Office Action, Claims 15 and 19 were rejected under § 103(a) as allegedly being unpatentable over Bialick et al. in view of Alexander et al. However, Alexander fails to remedy the shortcomings of Bialick discussed above to disclose or render obvious the invention of claim 1 upon which claims 15 and 19 depend, and for this

---

[2] M.P.E.P § 2143.

reason at least the rejection based on the combination of Bialick and Alexander should be withdrawn.

CONCLUSION

In view of the foregoing, Applicant believes all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 408-282-1857.

Respectfully submitted,

Dated: 11/15/05

Khaled Shami
Reg. No. 38,745

THELEN REID & PRIEST LLP
P.O. Box 640640
San Jose, CA 95164-0640
(408) 282-1857 Telephone
(408) 287-8040 Facsimile